REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed January 24, 2006. Reconsideration and allowance of the application and presently pending claims are respectfully requested.

1. Amendments to the Specification

Applicants have amended portions of the specification, as previously indicated. It is believed that the following amendments add no new matter to the present application.

2. Response to Rejection of Claims 1-10, 12-16, and 18-21 Under 35 U.S.C. §103(a)

In the Office Action, claims 1-10, 12-16, and 18-21 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Lagarde* (U.S. Patent No. 5,721,908) in view of *Smith* (U.S. Patent No. 6,151,675) in further view of *Vanstone* (U.S. Patent No. 6,134,325). It is well-established at law that, for a proper rejection of a claim under 35 U.S.C. §103 as being obvious based upon a combination of references, the cited combination of references must disclose, teach, or suggest, either implicitly or explicitly, all elements/features/steps of the claim at issue. *See, e.g., In Re Dow Chemical*, 5 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1988), and *In re Keller*, 208 U.S.P.Q.2d 871, 881 (C.C.P.A. 1981).

a. Claim 1

As provided in independent claim 1, Applicants claim:

From a user's browser, a secure method of image production in a web-based imaging environment, said method comprising the steps of:
accessing a destination web service;
downloading into said browser web content associated with said accessed destination web service;
downloading into said browser a public encryption key from said accessed destination web service;
retrieving image data under control of said browser;
encrypting said retrieved image data, wherein said downloaded public encryption key is utilized as part of said encrypting step;

BEST AVAILABLE COPY

-8-

transmitting said encrypted image data to said accessed destination web service; and

decrypting said encrypted image data by said accessed destination web service, wherein a private encryption key counterpart of said public encryption key is utilized as part of said decrypting step, said private encryption key being accessible exclusively to said accessed destination web service.

(Emphasis added).

In the present case, the cited art does not teach or suggest all of the claim limitations, and there is no suggestion or motivation in the cited art to modify the references to include those limitations. For example, neither *Lagarde* nor *Smith* teaches or suggests "downloading into said browser a public encryption key <u>from said accessed destination web service</u>," as recited and emphasized above in claim 1. (Emphasis added). For example, *Smith* teaches "encrypt[ing] the document with the public key of a server associated with the recipient of the document, <u>instead of encrypting the document with the public key of the intended recipient</u>." Col. 4, lines 4-7 (Emphasis added). To encrypt the document with the public encryption key of an intended recipient, such as a destination web service, *Smith* teaches that the encrypted document would have to be decrypted and then reencrypted by the DDCS server utilizing the public encryption key of the recipient. *See* col. 6, lines 48-60.

Therefore, *Smith* is devoid of a teaching for downloading a public encryption key of a destination web service into a browser, since *Smith* discloses that the public key of an intended recipient is <u>not</u> provided to a browser. Moreover, *Smith* teaches that the approach of not providing a public key of an intended recipient to a browser is preferred over an approach where a public key of a destination web service is provided to a browser. In particular, *Smith* clearly states that "<u>instead of encrypting the document with the public key of the intended recipient</u>," the document is encrypted "with the public key of a server associated with the recipient of the document." Col. 4, lines 4-7 (Emphasis added). Hence, to modify, the teachings of *Smith* to include the feature of "downloading into said browser a public encryption key from said accessed destination web service" is contrary to the teachings of *Smith*.

As a result, it would <u>not be obvious</u> to combine *Smith* with a reference (*e.g.*, *Vanstone*) that allegedly teaches encrypting a document with a public key of an intended recipient, since *Smith* provides no motivation for doing so and clearly

-9-

teaches away from such. *See ACS Hospital Systems, Inc., v. Montefiore Hospital*, 732 F.2d 1572, 1577; 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) ("Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under section 103, teachings of references can be combined *only* if there is some suggestion or incentive to do so."). *See also ALCO Standard Corp. v. Tennessee Valley Authority*, 808 F.2d 1490, 1498, 1 U.S.P.Q.2d 1337, 1343 (Fed. Cir. 1986) ("Moreover, the question is not simply whether the prior art 'teaches' the particular element of the invention, but whether it would 'suggest the desirability, and thus the obviousness, of making the combination.'"); *Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Co.*, 730 F.2d 1452, 1462, 221 U.S.P.Q. 481 (Fed. Cir. 1984) ("The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.").

Therefore, a prima facie case establishing an obviousness rejection has not been made by the proposed combination of *Lagarde* in view of *Smith* in further view of *Vanstone*. Thus, claim 1 is not obvious in view of the cited references, and the rejection should be withdrawn for at least this reason alone.

b. Claims 2-10

Because independent claim 1 is allowable over the cited art of record, dependent claims 2-10 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that the dependent claims contain all the steps and features of independent claim 1. For at least this reason, the rejection of claims 2-10 should be withdrawn.

c. Claim 12

As provided in independent claim 12, Applicants claim:

> A computer for providing secure image production in a web-based imaging environment, said computer operable to:
> access a destination web service;
> download web content from said destination web service to a user's browser;

-10-

> download a public encryption key from said destination web
> service to the user's browser;
>
> encrypt imaging data using said public encryption key as part
> of encryption process;
>
> transmit said encrypted imaging data to said destination web
> service; and
>
> direct said destination web service to decrypt said encrypted
> imaging data using a private encryption key counterpart of said public
> encryption key as part of decryption process, said private encryption
> key being accessible exclusively to said destination web service.

(Emphasis added).

In the present case, the cited art does not teach or suggest all of the claim limitations, and there is no suggestion or motivation in the cited art to modify the references to include those limitations. For example, neither *Lagarde* nor *Smith* teaches or suggests "download[ing] a public encryption key <u>from said destination web service to the user's browser</u>," as recited in claim 12. (Emphasis added). For example, *Smith* teaches "encrypt[ing] the document with the public key of a server associated with the recipient of the document, <u>instead of encrypting the document with the public key of the intended recipient</u>." Col. 4, lines 4-7 (Emphasis added). To encrypt the document with the public encryption key of an intended recipient, such as a destination web service, *Smith* teaches that the encrypted document would have to be decrypted and then reencrypted by the DDCS server utilizing the public encryption key of the recipient. *See* col. 6, lines 48-60. Therefore, *Smith* is devoid of a teaching for downloading a public encryption key of a destination web service into a browser, since *Smith* discloses that the public key of an intended recipient is <u>not</u> provided to a browser. Moreover, *Smith* teaches that the approach of not providing a public key of an intended recipient to a browser is preferred over an approach where a public key of a destination web service is provided to a browser. In particular, *Smith* clearly states that "<u>instead of encrypting the document with the public key of the intended recipient</u>," a document is encrypted "with the public key of a server associated with the recipient of the document." Col. 4, lines 4-7 (Emphasis added). Thus, to modify, the teachings of *Smith* to include the feature of "download[ing] a public encryption key from said destination web service to the user's browser" is in opposition to the teachings of *Smith*.

-11-

As a result, it would <u>not be obvious</u> to combine *Smith* with a reference (*e.g.,* *Vanstone*) that allegedly teaches encrypting a document with a public key of an intended recipient, since *Smith* provides no motivation for doing so and clearly teaches away from such. *See ACS Hospital Systems, Inc., v. Montefiore Hospital*, 732 F.2d 1572, 1577; 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) ("Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under section 103, teachings of references can be combined *only* if there is some suggestion or incentive to do so."). *See also ALCO Standard Corp. v. Tennessee Valley Authority*, 808 F.2d 1490, 1498, 1 U.S.P.Q.2d 1337, 1343 (Fed. Cir. 1986) ("Moreover, the question is not simply whether the prior art 'teaches' the particular element of the invention, but whether it would 'suggest the desirability, and thus the obviousness, of making the combination.'"); *Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Co.*, 730 F.2d 1452, 1462, 221 U.S.P.Q. 481 (Fed. Cir. 1984) ("The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.").

Therefore, a prima facie case establishing an obviousness rejection <u>has not</u> been made by the proposed combination of *Lagarde* in view of *Smith* in further view of *Vanstone*. Thus, claim 12 is not obvious in view of the cited references, and the rejection should be withdrawn for at least this reason alone.

d.   <u>Claims 13-16</u>

Because independent claim 12 is allowable over the cited art of record, dependent claims 13-16 (which depend from independent claim 12) are allowable as a matter of law for at least the reason that the dependent claims contain all the elements and features of independent claim 12. For at least this reason, the rejection of claims 13-16 should be withdrawn.

e.   Claim 18

As provided in independent claim 18, Applicants claim:

> A system for providing secure image production in a web-based imaging environment, said system comprising:
> a user's browser operable to encrypt image data using a first encryption key as part of encryption process and to transmit said encrypted image data;
> *a destination web service representing a production device, said web service operable to download said first encryption key into said user's browser, said destination web service further operable to receive said transmitted encrypted image data and to decrypt said received encrypted image data using a private encryption key counterpart of said first encryption key as part of decryption process;* and
> a data path interconnecting said user's browser with said destination web service.

(Emphasis added).

In the present case, the cited art does not teach or suggest all of the claim limitations, and there is no suggestion or motivation in the cited art to modify the references to include those limitations. For example, neither *Lagarde* nor *Smith* teaches or suggests "a destination web service representing a production device, said web service operable to download said first encryption key into said user's browser, said destination web service further operable to receive said transmitted encrypted image data and to decrypt said received encrypted image data using a private encryption key counterpart of said first encryption key as part of decryption process," as recited in claim 18.

For example, *Smith* teaches "encrypt[ing] the document with the public key of a server associated with the recipient of the document, instead of encrypting the document with the public key of the intended recipient." Col. 4, lines 4-7 (Emphasis added). To encrypt the document with the public encryption key of an intended recipient, such as a destination web service, *Smith* teaches that the encrypted document would have to be decrypted and then reencrypted by the DDCS server utilizing the public encryption key of the recipient. *See* col. 6, lines 48-60. Therefore, *Smith* is devoid of a teaching for downloading a public encryption key of a destination web service into a browser, since *Smith* discloses that the public key of an intended recipient is not provided to a browser. Moreover, *Smith* teaches that the

-13-

approach of not providing a public key of an intended recipient to a browser is preferred over an approach where a public key of a destination web service is provided to a browser. In particular, *Smith* clearly teaches "encrypt[ing] the document with the public key of a server associated with the recipient of the document, **instead of encrypting the document with the public key of the intended recipient**." Col. 4, lines 4–7 (Emphasis added). Hence, to modify, the teachings of *Smith* to include the feature of "a destination web service representing a production device, said web service operable to download said first encryption key into said user's browser, said destination web service further operable to receive said transmitted encrypted image data and to decrypt said received encrypted image data using a private encryption key counterpart of said first encryption key as part of decryption process" would teach away from *Smith*.

As a result, it would not be obvious to combine *Smith* with a reference (*e.g.*, *Vanstone*) that allegedly teaches encrypting a document with a public key of an intended recipient, since *Smith* provides no motivation for doing so and clearly teaches away from such. *See ACS Hospital Systems, Inc., v. Montefiore Hospital*, 732 F.2d 1572, 1577; 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) ("Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under section 103, teachings of references can be combined *only* if there is some suggestion or incentive to do so."). *See also ALCO Standard Corp. v. Tennessee Valley Authority*, 808 F.2d 1490, 1498, 1 U.S.P.Q.2d 1337, 1343 (Fed. Cir. 1986) ("Moreover, the question is not simply whether the prior art 'teaches' the particular element of the invention, but whether it would 'suggest the desirability, and thus the obviousness, of making the combination.'"); *Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Co.*, 730 F.2d 1452, 1462, 221 U.S.P.Q. 481 (Fed. Cir. 1984) ("The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.").

Therefore, a prima facie case establishing an obviousness rejection has not been made by the proposed combination of *Lagarde* in view of *Smith* in further view of *Vanstone*. Thus, claim 18 is not obvious in view of the cited references, and the rejection should be withdrawn for at least this reason alone.

-14-

f.   Claims 19-21

Because independent claim 18 is allowable over the cited art of record, dependent claims 19-21 (which depend from independent claim 18) are allowable as a matter of law for at least the reason that the dependent claims contain all the elements and features of independent claim 18. For at least this reason, the rejection of claims 19-21 should be withdrawn.

3.   Response to Rejection of Claims 11, 17, and 22 Under 35 U.S.C. §103(a)

In the Office Action, claims 11, 17, and 22 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Lagarde* in view of *Smith* in further view of *Applied Cryptography* by Bruce Schneier.

As noted above, claims 1, 12, and 18 are allowable over the cited art of record. Furthermore, Applicants finds nothing in *Applied Cryptography* to remedy the deficiencies of the cited art regarding claims 1, 12, and 18. Therefore, claims 11, 17, and 22 which depend from respective independent claims 1, 12, and 18 are also allowable.
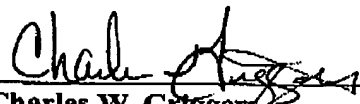
Additionally and notwithstanding the foregoing reasons for allowability of claims 11, 17, and 22, these claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Accordingly, the rejections to these claims should be withdrawn.

-15-

CONCLUSION

In light of the foregoing amendments and for at least the reasons set forth above, Applicants respectfully submit that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned agent at (770) 933-9500.

Respectfully submitted,

Charles W. Grigger
Reg. No. 47,283

-16-